WHAT IS CLAIMED IS:

1. A method of reconstructing a secret in a secret sharing scheme that generates n first shares from the secret information, n being an integer equal to or greater than two, the n shares being distributed to a group having n members in such a way that the original secret information can be reconstructed by a collection of any t members ($2 \leq t \leq n$), wherein:

each member among the t members uses the secret sharing scheme to generate t second shares from its first share, and distributes them to the t members;

each member among the t members performs a distributed computation by using the second share generated by the member and the $t - 1$ second shares received from the other members, the t members thereby generating t intermediate results; and

the original secret information is reconstructed from the t intermediate results.

2. The method of claim 1, wherein the secret sharing scheme generates the n first shares in such a way that the original secret information is a sum of the n first shares.

3. The method of claim 1, wherein the secret sharing scheme generates the second shares in such a way that a first share is a sum of all the second shares generated from the first share.

4. The method of claim 1, wherein the intermediate result generated by a member is a sum of the second share generated by the member and the $t - 1$ second shares received by the member.

5. The method of claim 1, wherein the n first shares are generated by a threshold secret sharing scheme using member IDs to identify each of the members.

6. The method of claim 1, wherein the second shares are generated from the first share held by each of the t members by using a threshold secret sharing scheme using member IDs or by using a secret sharing scheme that can reconstruct the secret by summing all shares.

7. The method of claim 1, wherein a member generates the intermediate result as a linear combination of the second share generated by the member and the t − 1. second shares received by the member, using coefficients based on member IDs.

8. The method of claim 1, further comprising a step of generating and distributing mutually distinct temporary member IDs to the t members, wherein:

the intermediate results for reconstructing the original secret information are calculated by a distributed computation using the temporary member IDs; and

the original secret information is reconstructed from the intermediate results and the temporary member IDs.

9. The method of claim 1, further comprising a step of generating third shares from the member IDs of the t members by using a secret sharing scheme, and distributing them to the t members.

10. A shared secret reconstruction apparatus for reconstructing a secret in a secret sharing scheme that generates n first shares from the secret information, n being an integer equal to or greater than two, the n shares

being distributed to a group having n members in such a way that the original secret information can be reconstructed by a collection of any t members ($2 \leq t \leq n$) separately possessing the shared secret reconstruction apparatus, the shared secret reconstruction apparatus thus operating together with $t - 1$ other shared secret reconstruction apparatuses, the shared secret reconstruction apparatus comprising:

a secret sharing operation unit generating second shares from a first share held by the shared secret reconstruction apparatus by using a secret sharing scheme and distributing the second shares to the t shared secret reconstruction apparatuses of the collected members;

a secret reconstruction operation unit calculating an intermediate result for reconstructing the original secret information in a distributed computation by use of the output from the secret sharing operation unit and the second shares received from the $t - 1$ other shared secret reconstruction apparatuses and transmitting the intermediate result.

11. A shared secret reconstruction apparatus for reconstructing a secret in a secret sharing scheme that generates n first shares from the secret information, n being an integer equal to or greater than two, the n shares being distributed to a group having n members in such a way that the original secret information can be reconstructed by a collection of any t members ($2 \leq t \leq n$) separately possessing the shared secret reconstruction apparatus, the shared secret reconstruction apparatus thus operating together with $t - 1$ other shared secret reconstruction apparatuses, the shared secret reconstruction apparatus comprising:

a secret sharing operation unit generating second

shares from a first share held by the shared secret reconstruction apparatus by using a secret sharing scheme and distributing them to the t - 1 other shared secret reconstruction apparatuses;

a secret reconstruction operation unit calculating an intermediate result for reconstructing the original secret information in a distributed computation by use of the output from the secret sharing operation unit and the second shares received from the t - 1 other shared secret reconstruction apparatuses; and

a secret reconstruction unit reconstructing the original secret information from the output from the secret reconstruction operation unit and the outputs received from the t - 1 other shared secret reconstruction apparatuses.

12. The shared secret reconstruction apparatus of claim 10, further comprising a secret reconstruction unit reconstructing the original secret information from the output from the secret reconstruction operation unit and the outputs received from the t - 1 other shared secret reconstruction apparatuses.

13. The shared secret reconstruction apparatus of claim 10, wherein the secret sharing scheme generates shares in such a way that the original secret information is a sum of all the shares.

14. The shared secret reconstruction apparatus of claim 10, wherein the secret reconstruction operation unit comprises an adder summing the output from the secret sharing operation unit and the second shares received from the t - 1 other shared secret reconstruction apparatuses.

15. The shared secret reconstruction apparatus of claim 10,

wherein the secret sharing operation unit uses a threshold secret sharing scheme using member IDs.

16. The shared secret reconstruction apparatus of claim 10, wherein the secret reconstruction operation unit comprises a linear combination operation unit performing a linear combination operation on the output from the secret sharing operation unit and the second shares received from the t - 1 other shared secret reconstruction apparatuses using coefficients calculated from the member IDs, the second shares being received via secure channels.

17. The shared secret reconstruction apparatus of claim 10, wherein the secret sharing operation unit uses a threshold secret sharing scheme using temporary member IDs distributed to the shared secret reconstruction apparatus.

18. The shared secret reconstruction apparatus of claim 10, wherein the secret sharing operation unit generates third shares from the member ID held by the shared secret reconstruction apparatus by using a secret sharing scheme and distributes them to the t - 1 other shared secret reconstruction apparatuses, the secret reconstruction operation unit thereby calculating an intermediate result for the secret reconstruction in the distributed computation by use of the second and third shares output from the secret sharing operation unit and received from the t - 1 other shared secret reconstruction apparatuses.

19. The shared secret reconstruction apparatus of claim 18, wherein the secret reconstruction operation unit comprises:

a term calculation unit performing a distributed multiplication on the result of a distributed computation performed on a coefficient calculated from the third share

to the second share and on this second share by use of the second and third shares output from the secret sharing operation unit and received from the t − 1 other shared secret reconstruction apparatuses; and

an adder summing all the outputs from the term calculation unit.

20. The shared secret reconstruction apparatus of claim 19, wherein the term calculation unit comprises:

a difference operation unit calculating differences between the different third shares;

a first multiple term distributed multiplication unit performing a distributed multiplication on the outputs from the difference operation unit;

a distributed inverse element calculation unit performing a distributed computation on the inverse element of the output from the first multiple term distributed multiplication unit;

a second multiple term distributed multiplication unit performing a distributed multiplication on the third shares; and

a pair of two term distributed multiplication units performing a distributed multiplication on the output from the distributed inverse element calculation unit, the output from the second multiple term distributed multiplication unit and the corresponding second share.

21. The shared secret reconstruction apparatus of claim 20, wherein each of the first and second multiple term distributed multiplication units comprises a number of two term distributed multiplication units each performing a distributed multiplication on two values, the number being one less than the number of values on which the distributed multiplication is performed.

22. The shared secret reconstruction apparatus of claim 21, wherein each of the two term distributed multiplication units comprises:

a multiplication unit multiplying two inputs;

a secret sharing unit generating fourth shares from the output from the multiplication unit by using a threshold secret sharing scheme using temporary member IDs and distributing them to the t − 1 other shared secret reconstruction apparatuses via secure channels; and

a linear combination operation unit performing a linear combination operation on the output from the secret sharing unit and the fourth shares received from the t − 1 other shared secret reconstruction apparatuses, using coefficients calculated from the temporary member IDs via the secure channels.

23. The shared secret reconstruction apparatus of claim 21, wherein each of the two term distributed multiplication units comprises:

a first multiplication units each multiplying two inputs together and then multiplying the product by a coefficient calculated from temporary member IDs;

first communication operation units each multiplying a first input to itself and a second input to a corresponding term distributed multiplication unit in another shared secret reconstruction apparatus by performing an oblivious transfer via the secure channels;

second communication operation units each multiplying a second input to itself and a first input to a corresponding term distributed multiplication unit in another shared secret reconstruction apparatus by performing an oblivious transfer via the secure channels;

first adders each summing the outputs from the first

and second communication operation units;

second multiplication units each multiplying the output from one of the first adders by a coefficient calculated from temporary member IDs; and

a second adder summing all the results of the first and second multiplication units.

24. The shared secret reconstruction apparatus of claim 21, wherein each of the two term distributed multiplication unit comprises:

a first multiplication unit multiplying first and second inputs to itself;

first communication operation units each multiplying the first input to itself and a second input to a corresponding term distributed multiplication unit in another shared secret reconstruction apparatuses by performing an oblivious transfer via the secure channels;

second communication operation units each multiplying the second input to itself and a first input to a corresponding term distributed multiplication unit in another shared secret reconstruction apparatus by performing an oblivious transfer via the secure channels;

first adders each summing the outputs from the first and second communication operation units; and

a second adder summing all the results of the first multiplication unit and the first adders.

25. The shared secret reconstruction apparatus of claim 20, wherein the distributed inverse element calculation unit comprises:

a number of distributed multiplication units performing a distributed multiplication on two values, the number being calculated from a size of a finite field used in the distributed multiplication; and

a multiple term distributed multiplication unit performing distributed multiplication on a number of values calculated from the size of the finite field used in the distributed multiplication, the multiple term distributed multiplication unit including a number of two term distributed multiplication unit performing a distributed multiplication on two values, the number of the two term distributed multiplication unit being one less than the number of values on which the distributed multiplication is performed.

26. The shared secret reconstruction apparatus of claim 20, wherein the distributed inverse element calculation unit comprises:

a random number generation unit generating a random number;

a first two term distributed multiplication unit performing a distributed multiplication on a first value and the output from the random number generation unit;

a linear combination operation unit performing a linear combination operation on the output from the first two term distributed multiplication unit and output received from the corresponding two term distributed multiplication unit in the t - 1 other shared secret reconstruction apparatuses, using coefficients calculated from temporary member IDs, the output being received via a secure channel;

an inverse element operation unit calculating the inverse element of the output from the linear combination operation unit in the finite field;

a secret sharing unit generating fifth shares from the output from the inverse element operation unit and distributing them to the t - 1 other shared secret reconstruction apparatuses via secure channels; and

a second two term distributed multiplication unit

receiving the fifth share from the secret sharing unit and the output from the random number generation unit as inputs and having the same structure as the first two term distributed multiplication unit.

27. The shared secret reconstruction apparatus of claim 20, wherein the distributed inverse element calculation unit comprises:

a random number generation unit generating a random number;

a first two term distributed multiplication unit performing a distributed multiplication on a first value and the output from the random number generation unit;

an adder summing the output from the first two term distributed multiplication unit and the outputs received from the corresponding first two term distributed multiplication unit in the t - 1 other shared secret reconstruction apparatuses, the outputs being received via secure channels;

an inverse element operation unit calculating the inverse element of the output from the adder in the finite field;

a secret sharing unit generating fifth shares from the output from the inverse element operation unit and distributing them to the t - 1 other shared secret reconstruction apparatuses via secure channels; and

a second two term distributed multiplication unit receiving the fifth share from the secret sharing unit and the output from the random number generation unit as inputs and having the same structure as the first two term distributed multiplication unit.

28. The shared secret reconstruction apparatus of claim 20, wherein the distributed inverse element calculation unit

comprises:

a random number generation unit generating a random number;

a first two term distributed multiplication unit performing a distributed multiplication on a first value and the output from the random number generation unit;

a transmission unit transmitting the result of the first two term distributed multiplication unit to a shared secret reconstruction apparatus;

a receiving unit for receiving the fifth share from the shared secret reconstruction apparatus; and

a second two term distributed multiplication unit performing a distributed multiplication on the received fifth share and the output from the random number generation unit.

29. A secret reconstruction system for carrying out a secret reconstruction method for reconstructing a secret in a secret sharing scheme that generates n first shares from the secret information, n being an integer equal to or greater than two, the n shares being distributed to a group having n members in such a way that the original secret information can be reconstructed by a collection of any t members ($2 \leq t \leq n$), the secret reconstruction system comprising:

a plurality of shared secret reconstruction apparatuses as described in claim 10; and

a secret reconstruction apparatus reconstructing the original secret information from the outputs of the plurality of shared secret reconstruction apparatuses.

30. The secret reconstruction system of claim 29, wherein the secret reconstruction apparatus is included in one of the plurality of shared secret reconstruction apparatuses.

31. The secret reconstruction system of claim 29, wherein the secret reconstruction apparatus reconstructs the original secret information by summing the outputs of all of the plurality of shared secret reconstruction apparatuses.

32. The secret reconstruction system of claim 29, wherein the secret reconstruction apparatus reconstructs the original secret information by using a reconstruction method of a threshold secret sharing scheme using temporary member IDs.

33. The secret reconstruction system of claim 29, further comprising a temporary member ID generation unit generating mutually distinct temporary member IDs to the shared secret reconstruction apparatuses operated by the collected members, and distributing and revealing them to the shared secret reconstruction apparatuses.

34. The secret reconstruction system of claim 33, wherein the first shares are generated in such a way that the original secret information is a sum of all the first shares.

35. The secret reconstruction system of claim 33, wherein the first shares are generated by using a threshold secret sharing scheme using member IDs.